UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/686,343	10/14/2003	Ernie Brickell	42P15784	7197

59796 7590 11/26/2007

INTEL CORPORATION
c/o INTELLEVATE, LLC
P.O. BOX 52050
MINNEAPOLIS, MN 55402

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
11/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/686,343	BRICKELL ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 9/12/07.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1,2,4-10,12-18 and 20 is/are pending in the application.

4a) Of the above claim(s) 3,11,19 is/are ~~withdrawn from consideration~~ canceled.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1,2,4-10,12-18 and 20 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-2, 4-10, 12-18, and 20 are pending.

Claims 3, 11, and 19 remains cancelled.

Response to Arguments

2. *Applicant's arguments filed 9/12/2007 have been fully considered but they are not persuasive.*

The amended claimed limitation "but not the master owner token" remains to read on the Scherr and Challener combination. Scherr discloses host tokens (delegate owner token) are distributed and used to identify and authenticate host computers (delegated environment). For the master token is not communicated to the host computers but the host tokens are distributed to the host environment which corresponds to the claimed communicating the delegate owner token, but not the master token, to the delegated environment (col.5, lines 52-53). Further, Challener discloses the system comprising a server (delegated environment) and the remote user password (delegate owner token) where the remote user password is given to the server and to the security chip (TPM) as claimed, rather than the master token being given to the server (col.4, lines 57-59). Therefore, the master token is not disclosed as being communicated to the delegated environment in the Scherr and Challener combination. Thus, Scherr and Challener read on the claimed invention.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-2, 4-10, 12-18, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable by Scherr, et al. (US 7,134,138), and further in view of Challener, et al. (US 7,194,762).

As per claim 1:

Scherr discloses a method of managing authorization tokens within a computer system comprising:

creating a master owner token **(col.7, lines 63-65)** indicating a management environment has full ownership of a trusted platform module within the computer system; **((col.5, lines 48-53 and col.7, lines 40-50; Scherr discloses a master token and that the data access manager creates and distributes tokens and host tokens used to identify and authenticate host computers.),**

creating a delegate owner token for a delegated environment; **(col.6, lines 49-50 and col.7, lines 18-21; Scherr discloses a host token is the claimed delegate owner that identifies the host in the request sent to authorize access to data (col.5, lines 49-50). The claimed delegated environment can broadly be**

interpreted as components, computers, systems, etc. according to the host token.)

communicating the delegate owner token, but not the master owner token, to the delegated environment; and **(col.5, lines 50-54)**

allowing the delegated environment access *[to the trusted platform module]* when the delegated environment presents the delegate owner token *[to the trusted platform module]*. **(col.13, lines 23-35 and col.14, lines 49-65)**

Scherr discloses host tokens (delegate owner token) are distributed and used to identify and authenticate host computers (delegated environment). For the master token is not communicated to the host computers but the host tokens are distributed to the host environment which corresponds to the claimed communicating the delegate owner token, but not the master token, to the delegated environment (col.5, lines 52-53). Scherr discloses creating a master token of a data access manager and allowing access to the data access manager rather than for a trusted platform module (TPM). Thus, Scherr did not include a TPM.

Challener discloses a method and system for improved security password-based access to computer networks. The system comprises a server where the server comprises a security chip (col.2, lines 45-49). The invention comprises a security chip, such as a Trusted Platform Module (TPM) where a phrase is signed by the security chip using an encryption key assigned either to the remote user or the security chip (col.2, lines 16-18 and 28-32). The security chip comprises encryption keys, such as a public key/private key pair assigned to the chip (col.2, lines 51-53). Challener discloses a

remote user request access to the computer network by providing an ID and password to the server (col.3, lines 4-7). The password is according to the remote user and for access to the server. Thus, the system comprising a server reads on the claimed delegated environment and the remote user password reads on the delegate owner token because the user's password is given to the server and to the security chip (TPM) as claimed (col.4, lines 57-59). Further, Challener discloses the system comprising a server (delegated environment) and the remote user password (delegate owner token) where the remote user password is given to the server as claimed, rather than the master token being given to the server (col.4, lines 57-59). Challener teaches using a security chip further decreases the exposure to brute force attacks and such TPM allow only certain number of unsuccessful entries of a password before a user is locked (col.3, lines 24-26). So the user of the security chip enforces protection against hardware hammering (col.4, lines 15-19).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching by Scherr of the master token to indicate full ownership and to allow access with the teaching of a trusted platform module (TPM) as taught by Challener because using a security chip decrease the exposure to brute force attacks and enforces protection against hardware hammering (col.3, lines 24-26 and col.4, lines 18-19).

As per claim 2: **See Scherr on col.8, lines 34-37;** discloses the method of claim 1, further comprising storing the master owner token in a secure storage within the computer system.

As per claim 3: **Cancelled**

As per claim 4: **See Scherr on col.5, lines 50-54;** discloses the method of claim 1, wherein creating the delegate owner token comprises the management environment sealing the delegate owner token to the delegated environment.

As per claim 5: **See Scherr on col.7, lines 64-65;** discloses the method of claim 1, further comprising wherein the master owner token indicating the management environment can change at least one of the master owner token and a delegate owner token.

As per claim 6: **See Scherr on col.5, lines 31-36;** discloses the method of claim 1, further comprising launching the management environment and then launching the delegated environment.

As per claim 7: **See col.8, lines 22-25 and 62-64;** discloses the method of claim 1, further comprising storing the delegate owner token in an access control list in the resource.

As per claim 8: **See Scherr on col.12, lines 41-49;** discloses the method of claim 7, further comprising removing, by the management environment, the delegate owner token from the access control list and adding a different delegate owner token to the access control list.

As per claim 9:

Scherr discloses an article comprising:

a storage medium having a plurality of machine readable instructions, wherein when the instructions are executed by a processor **(col.6, lines 57-67)**, the instructions

provide for managing authorization tokens within a computer system by creating a master owner token **(col.7, lines 63-65)** indicating an administrative environment has full ownership *[of a trusted platform module]* within the computer system; **(col.5, lines 48-53 and col.7, lines 40-50; Scherr discloses a master token and that the data access manager creates and distributes tokens and host tokens used to identify and authenticate host computers.),**

creating a delegate owner token for a delegate environment; **(col.6, lines 49-50 and col.7, lines 18-21; Scherr discloses a host token is the claimed delegate owner that identifies the host in the request sent to authorize access to data (col.5, lines 49-50). The claimed delegated environment can broadly be interpreted as components, computers, systems, etc. according to the host token.)**

communicating the delegate owner token, but not the master owner token, to the delegated environment; and **(col.5, lines 50-54)**

allowing the delegated environment access *[to the trusted platform module]* when the delegated environment presents the delegate owner token *[to the trusted platform module]* **(col.13, lines 23-35 and col.14, lines 49-65)**

Scherr discloses host tokens (delegate owner token) are distributed and used to identify and authenticate host computers (delegated environment). For the master token is not communicated to the host computers but the host tokens are distributed to the host environment which corresponds to the claimed communicating the delegate owner token, but not the master token, to the delegated environment (col.5, lines 52-

53). Scherr discloses creating a master token of a data access manager and allowing access to the data access manager rather than for a trusted platform module (TPM). Thus, Scherr did not include a TPM.

Challener discloses a method and system for improved security password-based access to computer networks. The system comprises a server where the server comprises a security chip (col.2, lines 45-49). The invention comprises a security chip, such as a Trusted Platform Module (TPM) where a phrase is signed by the security chip using an encryption key assigned either to the remote user or the security chip (col.2, lines 16-18 and 28-32). The security chip comprises encryption keys, such as a public key/private key pair assigned to the chip (col.2, lines 51-53). Challener discloses a remote user request access to the computer network by providing an ID and password to the server (col.3, lines 4-7). The password is according to the remote user and for access to the server. Thus, the system comprising a server reads on the claimed delegated environment and the remote user password reads on the delegate owner token because the user's password is given to the server and to the security chip (TPM) as claimed (col.4, lines 57-59). Further, Challener discloses the system comprising a server (delegated environment) and the remote user password (delegate owner token) where the remote user password is given to the server as claimed, rather than the master token being given to the server (col.4, lines 57-59). Challener teaches using a security chip further decreases the exposure to brute force attacks and such TPM allow only certain number of unsuccessful entries of a password before a user is locked

(col.3, lines 24-26). So the user of the security chip enforces protection against hardware hammering (col.4, lines 15-19).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching by Scherr of the master token to indicate full ownership and to allow access with the teaching of a trusted platform module (TPM) as taught by Challener because using a security chip decrease the exposure to brute force attacks and enforces protection against hardware hammering (col.3, lines 24-26 and col.4, lines 18-19).

As per claim 10: **See Scherr on col.8, lines 34-37;** discloses the article of claim 9, further comprising instructions for storing the master owner token in a secure storage within the computer system.

As per claim 11: **Cancelled**

As per claim 12: **See Scherr on col.5, lines 50-54;** discloses the article of claim 9, wherein creating the delegate owner token comprises the administrative environment sealing the delegate owner token to the delegated environment.

As per claim 13: **See Scherr on col.7, lines 64-65;** discloses the article of claim 9, further comprising the master owner token indicating the administrative environment can change at least one of the master owner token and the delegate owner token.

As per claim 14: **See Scherr on col.5, lines 31-36;** discloses the article of claim 9, further comprising instructions for launching the administrative environment and then launching the delegated environment.

As per claim 15: **See Scherr on col.8, lines 22-25 and 62-64;** discloses the article

of claim 9, further comprising instructions for storing the delegate owner token in an access control list in the resource.

As per claim 16: See Scherr on col.12, lines 41-49; discloses the article of claim 9, further comprising instructions for removing, by the administrative environment, the delegate owner token from the access control list and adding a different delegate owner token to the access control list.

As per claim 17:

Scherr discloses a computer system comprising:

a plurality of delegated environments;

a management environment to create a master owner token **(col.7, lines 63-65)** indicating the management environment has full ownership *[of a trusted platform module]* within the computer system **(col.5, lines 48-53 and col.7, lines 40-50; Scherr discloses a master token and that the data access manager creates and distributes tokens and host tokens used to identify and authenticate host computers.),** to create a plurality of delegate owner tokens indicating partial ownership *[of the trusted platform module]* **(col.6, lines 49-50 and col.7, lines 18-21; Scherr discloses a host token is the claimed delegate owner that identifies the host in the request sent to authorize access to data (col.5, lines 49-50). The claimed delegated environment can broadly be interpreted as components, computers, systems, etc. according to the host token.)**, and to communicate a selected one of the plurality of delegate owner tokens, but not the master owner token, to a selected one of the plurality of delegated environments; **(col.5, lines 41-54)**

wherein *[the trusted platform module]* stores delegate owner tokens created by the management environment and allows the selected one of the plurality of delegated environments access *[to the trusted platform module]* when the selected one of the plurality of delegate owner tokens is presented *[to the trusted platform module]* by the selected one of the plurality of delegated environments. **(col.13, lines 23-35 and col.14, lines 49-65)**

Scherr discloses host tokens (delegate owner token) are distributed and used to identify and authenticate host computers (delegated environment). For the master token is not communicated to the host computers but the host tokens are distributed to the host environment which corresponds to the claimed communicating the delegate owner token, but not the master token, to the delegated environment (col.5, lines 52-53). Scherr discloses creating a master token of a data access manager that function as a master password (col.7, lines 63-64) and allowing access to the data access manager rather than for a trusted platform module (TPM). Thus, Scherr did not include a TPM.

Challener discloses a method and system for improved security password-based access to computer networks. The system comprises a server where the server comprises a security chip (col.2, lines 45-49). The invention comprises a security chip, such as a Trusted Platform Module (TPM) where a phrase is signed by the security chip using an encryption key assigned either to the remote user or the security chip (col.2, lines 16-18 and 28-32). The security chip comprises encryption keys, such as a public key/private key pair assigned to the chip (col.2, lines 51-53). Challener discloses a

remote user request access to the computer network by providing an ID and password to the server (col.3, lines 4-7). The password is according to the remote user and for access to the server. Thus, the system comprising a server reads on the claimed delegated environment and the remote user password reads on the delegate owner token because the user's password is given to the server and to the security chip (TPM) as claimed (col.4, lines 57-59). Further, Challener discloses the system comprising a server (delegated environment) and the remote user password (delegate owner token) where the remote user password is given to the server as claimed, rather than the master token being given to the server (col.4, lines 57-59). Challener teaches using a security chip further decreases the exposure to brute force attacks and such TPM allow only certain number of unsuccessful entries of a password before a user is locked (col.3, lines 24-26). So the user of the security chip enforces protection against hardware hammering (col.4, lines 15-19).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching by Scherr of the master token to indicate full ownership and to allow access with the teaching of a trusted platform module (TPM) as taught by Challener because using a security chip decrease the exposure to brute force attacks and enforces protection against hardware hammering (col.3, lines 24-26 and col.4, lines 18-19).

As per claim 18: See Scherr on col.8, lines 34-37; discloses a computer system of claim 17, further comprising a secure storage to store the master owner token.

As per claim 19: Cancelled

As per claim 20: See Scherr on col.5, lines 50-54; discloses the computer system of claim 19, wherein the trusted platform module comprises an access control list for storing the delegate owner tokens received from the management environment.

Conclusion

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2135